

ABSTRAK

Teknologi informasi saat ini sangat berperan penting dalam menunjang proses bisnis. Semakin pesatnya perkembangan teknologi informasi saat ini menjadikan informasi salah satu aset yang sangat penting dan sangat berharga bagi perusahaan. Seiring dengan meningkatnya nilai aset informasi, maka semakin besar keinginan orang untuk mendapatkan akses ke informasi dan mengendalikannya. Sehingga muncul ancaman dan risiko yang mungkin terjadi pada aset teknologi informasi. Tren yang berkembang saat ini bahwa beberapa perusahaan mulai mempertimbangkan proses dalam menjaga dan melindungi informasi yang merupakan prinsip dalam keamanan informasi. Namun, hadirnya teknologi informasi tidak pernah lepas dari potensi ancaman dan risiko dari berbagai jenis sumber. Sehingga, diperlukan suatu pendekatan untuk melakukan pengelolaan risiko secara memadai salah satunya dengan melakukan manajemen risiko teknologi informasi. LAPAN bandung menghadapi berbagai risiko. Risiko yang dihadapi oleh LAPAN meliputi keamanan aset, kontrol akses pengguna, dan sebagainya. Obyek penelitian ini yaitu di LAPAN bandung yang diketahui belum memiliki prosedur manajemen keamanan informasi untuk infrastruktur RDSA. Penelitian ini bertujuan untuk melakukan penilaian dan analisis risiko infrastruktur RDSA di LAPAN bandung. Penelitian ini menggunakan analisis kualitatif dan semi kuantitatif dengan metode studi kasus. Analisis risiko ini menggunakan pendekatan dari standar ISO/IEC 27005:2011.

Kata kunci : ISO/IEC 27005, manajemen risiko keamanan informasi, teknologi informasi



ABSTRACT

Current information technology plays an important role in supporting business processes. The rapid development of information technology today makes the information one asset that is very important and very valuable to the company. As the value of information assets, the greater the desire to gain access to information and control. So that emerging threats and risks that may occur in the information technology assets. A growing trend now that some company began to consider processes in maintaining and protecting information which is the principle in information security. However, the presence of information technology can never be separated from potential threats and risks of various types of sources. Thus, we need a risk management approach to perform adequately either by doing risk management information technology. LAPAN Bandung face a variety of risks. Risks faced by LAPAN include asset security, control user access, and so forth. The object of this research is in LAPAN Bandung is known does not have an information security management procedures for RDSA infrastructure. This study aims to conduct risk assessment and analysis infrastructure LAPAN RDSA in Bandung. This study uses qualitative and semi-quantitative analysis with the case study method. This risk analysis using the approach of the standard ISO / IEC 27 005: 2011

Keyword: information technology, ISO/IEC 27005, risk management security information



DAFTAR ISI

LEMBAR PENGESAHAN	i
PERNYATAAN ORISINALITAS LAPORAN PENELITIAN.....	ii
PERNYATAAN PUBLIKASI LAPORAN PENELITIAN	iii
PRAKATA.....	iv
ABSTRAK	vi
ABSTRACT.....	vii
DAFTAR ISI.....	viii
DAFTAR GAMBAR	xi
DAFTAR TABEL.....	xii
BAB 1 PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Tujuan Pembahasan	2
1.4 Ruang Lingkup.....	2
1.5 Sumber Data.....	3
1.6 Sistematika Penyajian	4
BAB 2 KAJIAN TEORI	5
2.1 Teknologi Informasi.....	5
2.2 Sistem Informasi	5
2.3 Manajemen Aset Informasi	5
2.4 Klasifikasi Aset	6
2.5 Keamanan Informasi	6
2.6 Ancaman Keamanan Informasi.....	7
2.7 Manajemen Keamanan Informasi	7

2.8 Konsep Manajemen Risiko	7
2.8.1 Pengertian Risiko	8
2.8.2 Macam-Macam Risiko	8
2.8.3 Penanggulangan Risiko	9
2.9 Kategori Risiko Teknologi Informasi	9
2.10 Pengertian Manajemen Risiko	10
2.10.1 Fungsi-Fungsi Pokok Manajemen Risiko	11
2.11 ISO/IEC 27005:2011.....	11
2.11.1 <i>Context Establishment</i>	13
2.11.2 <i>Information Security Risk Assessment</i>	16
2.11.3 <i>Risk Treatment</i>	18
2.11.4 <i>Information Security Risk Acceptance</i>	19
2.11.5 <i>Information Security Risk Communication</i>	19
2.11.6 <i>Information Security Risk Monitoring and Review</i>	19
2.12 Analisis Risiko Keamanan Informasi dengan <i>framework</i> ISO/IEC 27005:2011.....	20
BAB 3 ANALISIS DAN EVALUASI.....	24
3.1 LAPAN	24
3.1.1 Visi dan Misi.....	24
3.1.2 Tujuan	25
3.1.3 Sasaran Strategis	25
3.1.4 Arah Kebijakan	26
3.1.5 Strategi	26
3.1.6 Struktur Organisasi	29
3.1.7 RDSA	30
3.2 <i>Risk Analysis</i>	31

3.2.1 Risk Identification	31
3.2.2 Risk Estimation	76
3.3 Risk Evaluation	91
BAB 4 SIMPULAN DAN SARAN	97
4.1 Simpulan	97
4.2 Saran.....	98
DAFTAR PUSTAKA	99
LAMPIRAN A IDENTIFIKASI ASET SISTEM RDSA	A-1
LAMPIRAN B IDENTIFIKASI ANCAMAN ASET RDSA.....	B-1
LAMPIRAN C BUKTI FOTO	C-1
LAMPIRAN D Lembar Konfirmasi	D-1
LAMPIRAN E WAWANCARA	E-1
LAMPIRAN F KONTROL OBJEKTIF ISO/IEC 27001	F-1

DAFTAR GAMBAR

Gambar 2. 1 Proses Risiko Manajemen Informasi.....	12
Gambar 3. 1 Struktur Organisasi.....	29
Gambar 3. 2 Halaman Login.....	30
Gambar 3. 3 Data RDSA.....	31



DAFTAR TABEL

Tabel 2. 1 Ancaman Keamanan Informasi.....	7
Tabel 2. 2 Matriks Level Risiko.....	22
Tabel 3. 1 Parameter untuk <i>Asset Valuation</i>	34
Tabel 3. 2 Parameter untuk <i>Threat Valuation</i>	34
Tabel 3. 3 Parameter untuk <i>Vulnerability Valuation</i>	34
Tabel 3. 4 Daftar Aset Infrastruktur RDSA	37
Tabel 3. 5 Daftar Aset, Jenis Ancaman, dan Tingkatannya	41
Tabel 3. 6 Daftar Aset, Jenis Ancaman, Kerentanan dan Tingkatannya.....	52
Tabel 3. 7 Matriks <i>Level</i> Risiko	76
Tabel 3. 8 Hasil Penilaian Risiko.....	78
Tabel 3. 9 Pemetaan Risiko.....	92
Tabel 3. 10 Kontrol Rekomendasi Berdasarkan ISO/IEC 27001:2013	94